SECS1028 - Lab 6 - systemd-journald - Linux

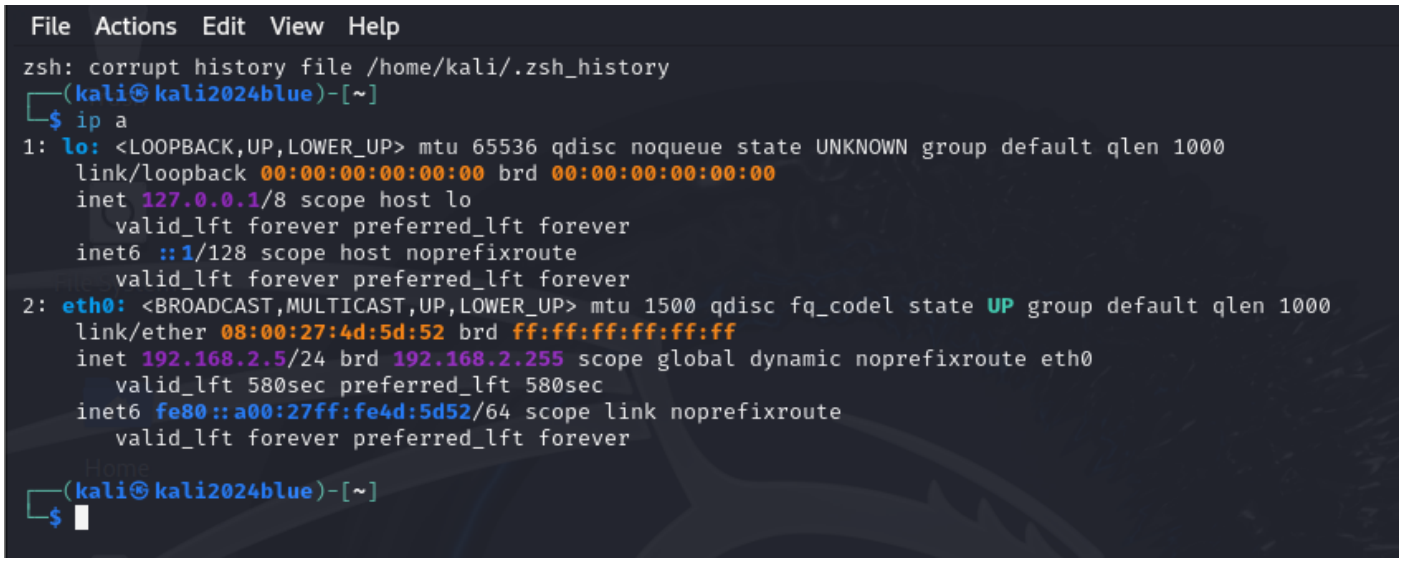
not´e sur 17 points - 10%

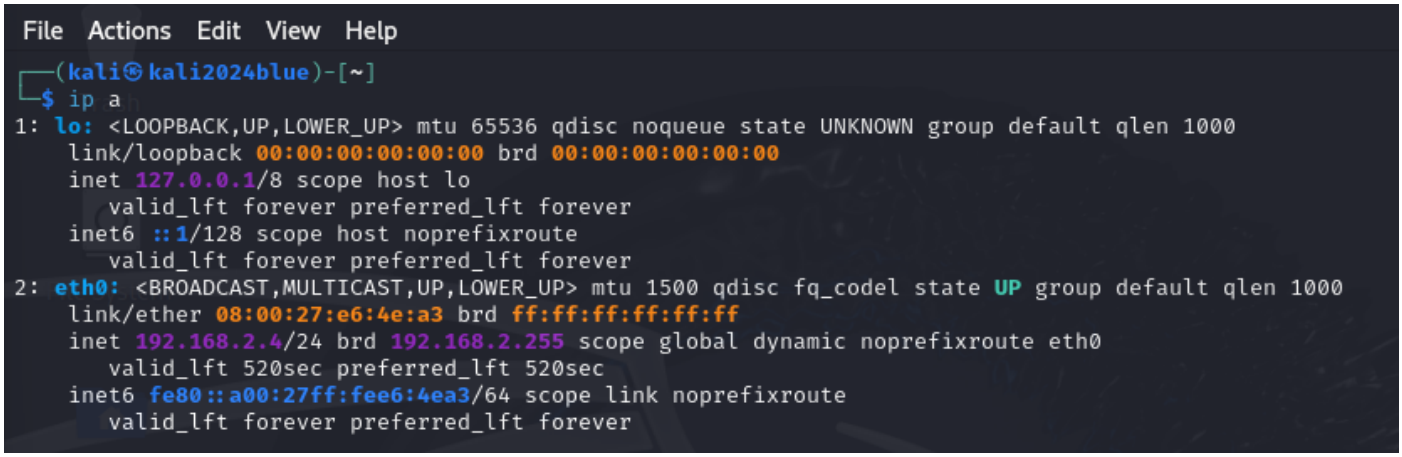
a` rendre pour le 17

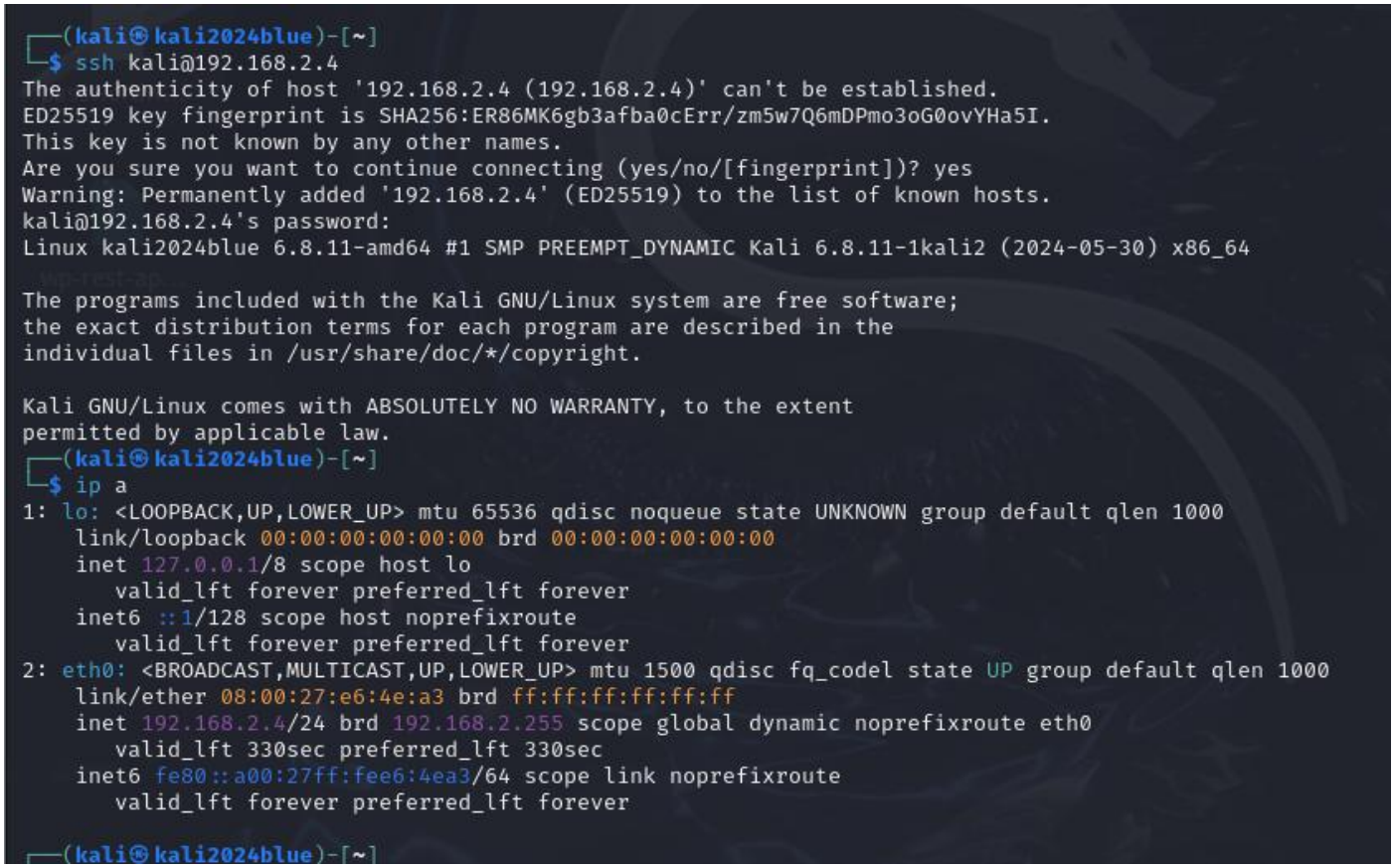
f´evrier

Objectif du laboratoire : manipuler les logs de systemd-journald.
Cr´edit pour la technique de manipulation du journal : https://unix.stackexchange.com/questions/272662/how-do-i-clear-journalctl-entries-for-a-specific-unit-only

Ce laboratoire n´ecessite deux VMs Kali connect´ees sur le r´eseau interne de Virtualbox. Choisissez une VM Kali (Kali 1) et clonez-la (Kali 2). Pour ce laboratoire, Kali 1 sera la machine d'attaque, Kali 2 la cible. Sur Kali 2, activez le service sshd (commande sudo systemctl start ssh). **Notez ci-dessous les adresses IP des deux VMs (1 point)** :







Vous devez ensuite utiliser uniquement la VM Kali 1 pour le laboratoire (connect´ee sur Kali 2 en ssh).

Vous devez ins´erer dans vos r´eponses des captures ´ecran illustrant celles-ci.

1 Systemd-journald (5 points)

1) Sous la VM kali 1, depuis le terminal, connectez-vous sous Kali 2 en ssh. Puis, sous ssh, affichez l'arborescence des processus en cours sur Kali 2 (pstree -p). Recherchez le processus systemdjournal. Quel est son PID ? Faites une capture ´ecran du PID. (1 point)

2) Sous la connexion ssh, testez la commande **journalctl -r**. Que fait-elle selon vous ? (1 point)

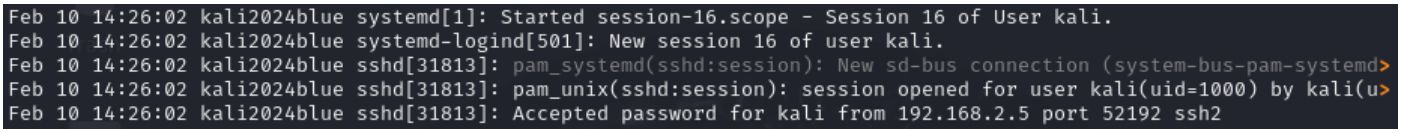
Elle met les plus récents logs donc les derniers logs rentrer (reverse)

```
└─$ journalctl -r
Feb 22 23:05:01 kali CRON[165905]: pam_unix(cron:session): session closed for user root
Feb 22 23:05:01 kali CRON[165907]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa111)
Feb 22 23:05:01 kali CRON[165905]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Feb 22 22:59:53 kali sudo[163420]: pam_unix(sudo:session): session closed for user root
Feb 22 22:59:53 kali sudo[163420]: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
Feb 22 22:59:53 kali sudo[163420]:    kali : TTY=pts/1 ; PWD=/tmp ; USER=root ; COMMAND=/usr/bin/journalctl>--
Feb 22 22:58:08 kali systemd[1]: NetworkManager-dispatcher.service: Deactivated successfully.
Feb 22 22:58:01 kali charon[85118]: 03[KNL] flags changed for fe80::20c:29ff:fe83:682c on eth0
Feb 22 22:58:01 kali NetworkManager[748]: <info>  [1740279481.2164] device (eth0): Activation: successful, devi>
Feb 22 22:58:01 kali NetworkManager[748]: <info>  [1740279481.2162] manager: NetworkManager state is now CONNEC
Feb 22 22:58:01 kali NetworkManager[748]: <info>  [1740279481.2161] device (eth0): state change: secondaries ->>
Feb 22 22:58:01 kali NetworkManager[748]: <info>  [1740279481.2160] device (eth0): state change: ip-check -> se>
Feb 22 22:58:01 kali NetworkManager[748]: <info>  [1740279481.2101] device (eth0): state change: ip-config -> i>
Feb 22 22:58:01 kali charon[85118]: 09[KNL] 192.168.3.3 appeared on eth0
Feb 22 22:58:01 kali NetworkManager[748]: <info>  [1740279481.2033] dhcp4 (eth0): state changed new lease, addr>
Feb 22 22:58:01 kali NetworkManager[748]: <info>  [1740279481.0074] dhcp4 (eth0): state changed new lease, addr>
Feb 22 22:57:59 kali NetworkManager[748]: <info>  [1740279479.9868] dhcp4 (eth0): state changed no lease
Feb 22 22:57:59 kali charon[85118]: 16[KNL] fe80::20c:29ff:fe83:682c appeared on eth0
Feb 22 22:57:59 kali NetworkManager[748]: <info>  [1740279479.9855] dhcp4 (eth0): activation: beginning transac>
Feb 22 22:57:59 kali NetworkManager[748]: <info>  [1740279479.9838] device (eth0): state change: config -> ip-c>
Feb 22 22:57:59 kali NetworkManager[748]: <info>  [1740279479.9830] device (eth0): state change: prepare -> con>
Feb 22 22:57:59 kali NetworkManager[748]: <info>  [1740279479.9829] manager: NetworkManager state is now CONNE
Feb 22 22:57:59 kali NetworkManager[748]: <info>  [1740279479.9828] device (eth0): state change: disconnected ->
Feb 22 22:57:59 kali NetworkManager[748]: <info>  [1740279479.9828] device (eth0): Activation: starting connect>
Feb 22 22:57:59 kali NetworkManager[748]: <info>  [1740279479.9825] policy: auto-activating connection 'Wired c>
Feb 22 22:57:59 kali NetworkManager[748]: <info>  [1740279479.9809] device (eth0): state change: unavailable ->>
```

3) Sous la connexion ssh, affichez la date et l'heure (commande date) de la VM Kali 2. Capture ´ecran. (0 point)

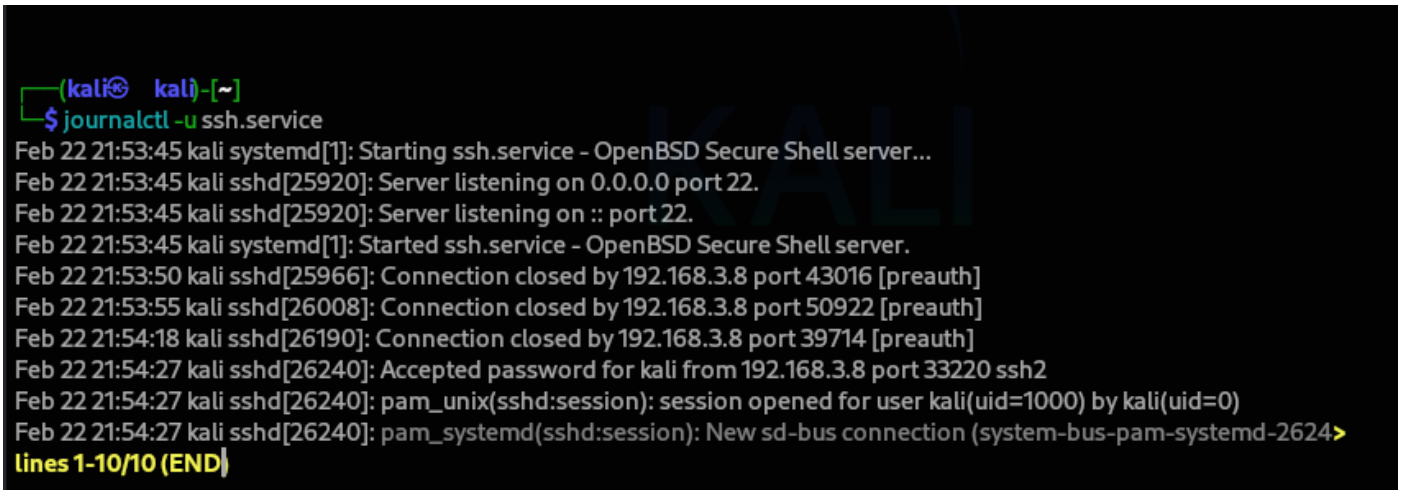
```
┌──(kali㉿kali2024blue)-[~]
└─$ date
Mon Feb 10 14:19:22 AST 2025
```

4) Dans quel fichier de kali 2 est stock´e l´´ev`enement que vous venez de cr´eer (connexion SSH) ? Combien de lignes ont ´et´e cr´e´ees pour cet ´ev`enement ? (capture ´ecran) (1 point)



1

5) Pouvez-vous afficher cet ´ev`enement avec la commande journalctl (**journalctl –help** pour les options) et trouver sa date ? (1 point)

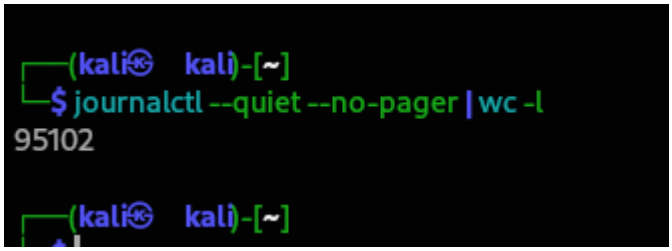


6) Pouvez-vous supprimer juste la (ou les) ligne contenant cet ev`enement dans ce fichier avec la commande journalctl ? Argumentez votre r´eponse. (1 point)

A l'aide d'une recherche j'ai remarque que ce n'est pas possible de supprimer la ligne que l'on veut, l'on peut seulement supprimer a partir d'une certaine date ou sinon le fichier en entier.

2 systemd-journald - suite (8 points)

1) Sous la connexion ssh sur Kali 2, quelle commande permet d'afficher le nombre de logs/´ev`enements dans le journal ? (1 point)

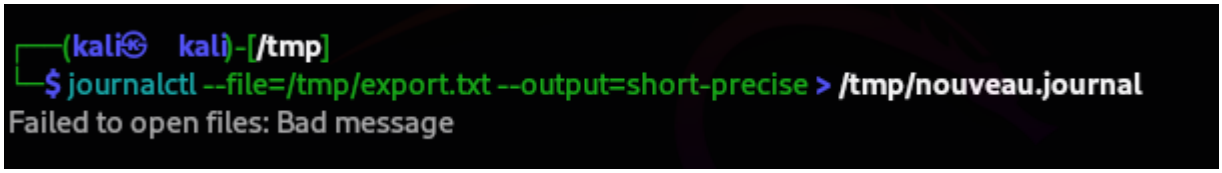


2) Sous la connexion ssh sur Kali 2, quelle commande permet d'exporter le journal au format texte ? Effectuez cette commande en nommant le fichier d'export "export.txt" dans le dossier /tmp de kali 2. (1 point)

3) Quelle commande permet d'exporter le journal au format texte ? Effectuez cette commande en nommant le fichier d'export "export.txt" dans le dossier /tmp. (1 point)

4) Recherchez et supprimez dans le fchier /tmp/export.txt les ´ev`enements post´erieurs a` la date que vous avez not´e. Vous vous aiderez pour cela du document suivant : https://systemd.io/JOURNAL_EXPORT_FORMATS/. (1 point)

5) Quelle commande permet de convertir un journal au format texte en un journal au format d'origine (binaire) ? Ex´ecutez cette commande en nommant et placant le fichier de sortie dans /tmp/nouveau.journal. (1 point)



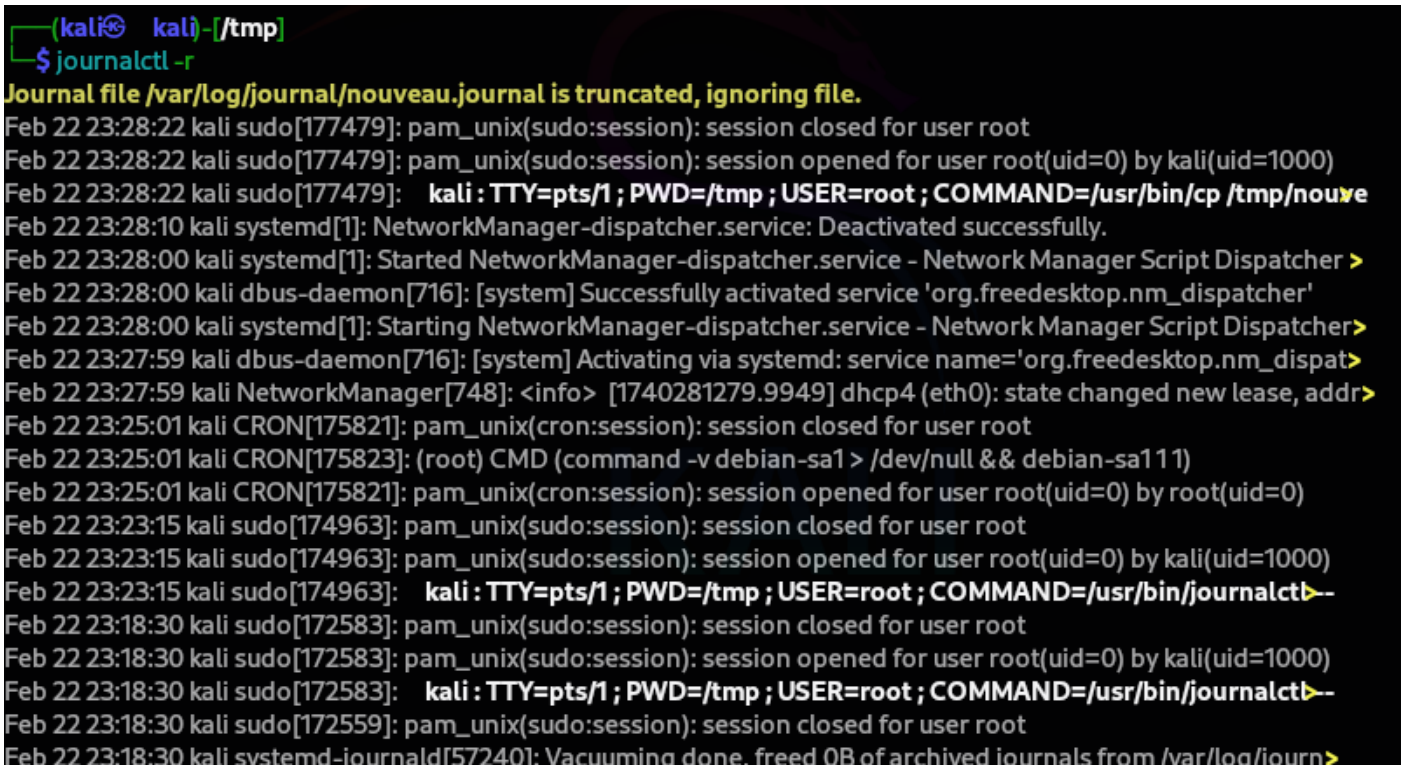
6) Supprimez tout le contenu du journal (de kali 2) avec la commande journalctl. Quelle est cette commande ? (1 point)

7) Remplacez le contenu du journal par le contenu du fichier /tmp/nouveau.journal. Affichez les derniers logs du journal (capture ´ecran). A quelle date correspondent-ils ? (1 point)

```
┌──(kali㉿kali)-[/tmp]
└─$ sudo cp /tmp/nouveau.journal /var/log/journal/
```

8) Avec la commande journalctl, affichez les logs du journal de Kali 2 dat´es entre une seconde de moins et une seconde de plus que la p´eriode de la partie 1 - question 5. Obtenez 1 point si l'objectif est atteint. (1 point)

Il y a quelque chose que jai mal fait mais bon jai essaye



3 Contre-mesures (3 points)

Quelle(s) contre-mesure(s) proposez-vous contre la manipulation du journal effectu´ee pr´ec´edemment ? (3 points)

Instaurer une journalisation sécurisée, configurer le systemd-journald pour rendre les journaux en lecture directement après leur écriture. Stocker les journaux a distance serait aussi une bonne façon d'empêcher la modification des journaux.

Fin du laboratoire.